# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-108148
(43)Date of publication of application : 24.04.1998

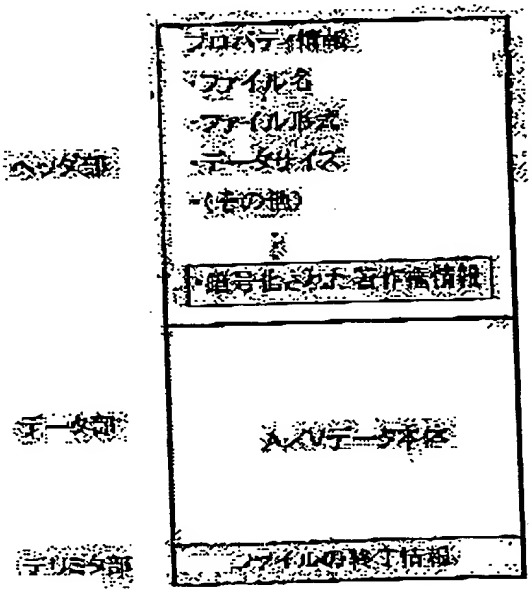
(51)Int.CL H04N 7/08
H04N 7/081
G06F 15/00
G09C 1/00
H04N 7/167

(21)Application number : 08-277130
(22)Date of filing : 27.09.1996

(71)Applicant : SONY CORP
(72)Inventor : KORI TERUHIKO

## (54) METHOD FOR PROTECTING COPYRIGHT OF DIGITAL DATA AND PROTECTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To protect the copyright of audio/vidual (A/V) data by providing copyright information to an A/V data file handled on a computer.
SOLUTION: Copyright information as file property information is stored to a header part of a file. The copyright information consists of file copy generation limit information and is encrypted by a prescribed encrypt key kc. In the case of accessing this file, at first, the copyright information is extracted from the header part. Since the copyright information cannot be decoded when the user accessing the file has no encrypt key kc, A/V data stored in the file are cannot be read. In the case of copying the file, since the copy generation limit information is rewritten and the rewritten copyright information is stored again, the copy generation is limited. Or the A/V data main body is encrypted by other encrypt key kd and the key kd is encrypted by the key kc with the copyright information, then the copyright is more surely protected.




LEGAL STATUS

[Date of request for examination] 14.03.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

---

## CLAIMS

---

[Claim(s)]
[Claim 1] The step of the encryption which enciphers copyright information in the protection-of-copyrights approach of the created digital data based on an encryption key, The step of copyright information storing which stores in the predetermined field of a file the copyright information by which encryption was carried out [ above-mentioned ], The protection-of-copyrights approach of the digital data which accesses to the above-mentioned file and is characterized by having the step of the decryption which decrypts the copyright information by which encryption was carried out [ above-mentioned ], and the step of the protection of copyrights which performs protection of copyrights based on the copyright information by which the decryption was carried out [ above-mentioned ].
[Claim 2] It is the protection-of-copyrights approach of the digital data characterized by being the field where the above-mentioned predetermined field stores the attribute information on the above-mentioned file in the protection-of-copyrights approach of digital data according to claim 1.
[Claim 3] It is the protection-of-copyrights approach of the digital data characterized by consisting of information to which the above-mentioned copyright information restricts the copy generation of the above-mentioned file in the protection-of-copyrights approach of digital data according to claim 1.
[Claim 4] It is the protection-of-copyrights approach of the digital data characterized by being saved even if the above-mentioned copyright information performs predetermined file manipulation to the above-mentioned file in the protection-of-copyrights approach of digital data according to claim 1.
[Claim 5] It is the protection-of-copyrights approach of the digital data characterized by making each of the step of the above-mentioned encryption, the step of the above-mentioned copyright information storing, the step of the above-mentioned decryption, and the step of the above-mentioned protection of copyrights on predetermined application software in the protection-of-copyrights approach of digital data according to claim 1.
[Claim 6] It is the protection-of-copyrights approach of the digital data characterized by making each of the step of the above-mentioned encryption, the step of the above-mentioned copyright information storing, the step of the above-mentioned decryption, and the step of the above-mentioned protection of copyrights on operation system in the protection-of-copyrights approach of digital data according to claim 1.
[Claim 7] It is the protection-of-copyrights approach of the digital data which is changed into the format corresponding to [ in case the digital A/V data obtained by carrying out predetermined file manipulation to the above-mentioned file in the protection-of-copyrights approach of digital data according to claim 1 are changed and transmitted to the signal of other formats ] a format besides the above in the above-mentioned copyright information, and is characterized by the above-mentioned thing done for transmission with the signal of a format besides the above.
[Claim 8] It is the protection-of-copyrights approach of digital data of having further the step of other encryption which enciphers the body of data of the above-mentioned file stored in the above-mentioned file based on other encryption keys in the protection-of-copyrights approach of digital data according to claim 1, and the step of the decryption of others which decrypts the

above-mentioned body of data based on an encryption key besides the above, and carrying out the step of the above-mentioned encryption enciphering the above-mentioned copyright information, and an encryption key besides the above with the above-mentioned encryption key as the description.
[Claim 9] It is the protection-of-copyrights approach of the digital data characterized by making each of the step of encryption of others [ above ], and the step of a decryption of others [ above ] on predetermined application software in the protection-of-copyrights approach of digital data according to claim 8.
[Claim 10] It is the protection-of-copyrights approach of the digital data characterized by making each of the step of encryption of others [ above ], and the step of a decryption of others [ above ] on operation system in the protection-of-copyrights approach of digital data according to claim 8.
[Claim 11] An encryption means to encipher copyright information in the copyright protection system of the created digital data based on an encryption key, A copyright information storing means to store in the predetermined field of a file the copyright information by which encryption was carried out [ above-mentioned ], The copyright protection system of the digital data which accesses to the above-mentioned file and is characterized by having a decryption means to decrypt the copyright information by which encryption was carried out [ above-mentioned ], and the copyright safeguard which performs protection of copyrights based on the copyright information by which the decryption was carried out [ above-mentioned ].
[Claim 12] It is the copyright protection system of the digital data characterized by being the field where the above-mentioned predetermined field stores the attribute information on the above-mentioned file in the copyright protection system of digital data according to claim 11.
[Claim 13] It is the copyright protection system of the digital data characterized by consisting of information to which the above-mentioned copyright information restricts the copy generation of the above-mentioned file in the copyright protection system of digital data according to claim 11.
[Claim 14] It is the copyright protection system of the digital data characterized by being saved even if the above-mentioned copyright information performs predetermined file manipulation to the above-mentioned file in the copyright protection system of digital data according to claim 11.
[Claim 15] It is the copyright protection system of the digital data characterized by predetermined application software having each of the above-mentioned encryption means, the above-mentioned copyright information storing means, the above-mentioned decryption means, and the above-mentioned copyright safeguard in the copyright protection system of digital data according to claim 11.
[Claim 16] It is the copyright protection system of the digital data characterized by operation system having each of the above-mentioned encryption means, the above-mentioned copyright information storing means, the above-mentioned decryption means, and the above-mentioned copyright safeguard in the copyright protection system of digital data according to claim 11.
[Claim 17] It is the copyright protection system of the digital data which is changed into the format corresponding to [ in case the digital A/V data obtained by carrying out predetermined file manipulation to the above-mentioned file in the copyright protection system of digital data according to claim 11 are changed and transmitted to the signal of other formats ] a format besides the above in the above-mentioned copyright information, and is characterized by the above-mentioned thing done for transmission with the signal of a format besides the above.
[Claim 18] It is the copyright protection system of the digital data have further other encryption means encipher the body of the above-mentioned file stored in the above-mentioned file of data in the copyright protection system of digital data according to claim 11 based on other encryption keys, and other decryption means decrypt the above-mentioned body of data based on an encryption key besides the above, and carry out that the above-mentioned encryption means enciphers the above-mentioned copyright information, and an encryption key besides the above with the above-mentioned encryption key as the description.
[Claim 19] It is the copyright protection system of the digital data characterized by predetermined application software having each of an encryption means besides the above, and a decryption means besides the above in the copyright protection system of digital data

according to claim 18.
[Claim 20] It is the copyright protection system of the digital data characterized by operation system having each of an encryption means besides the above, and a decryption means besides the above in the copyright protection system of digital data according to claim 18.

---

[Translation done.]

## DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention gives copyright information as attribute information on a data file, and relates to the protection-of-copyrights approach of digital data and a protection system which protect the copyright of the digital data created as a work by enciphering this copyright information based on a predetermined approach.
[0002]
[Description of the Prior Art] Improvement in the speed of recent years and a computer, large-capacity-izing of a digital recording medium, development of a computer network, development of image compression technology, etc. are **** better **. CG created by the digitized video signal, the sound signal, or computer in connection with it (Computer Graphics) A work etc. is A/V (Audio/Video). What is recorded as a data file is performed. In this way, the recorded A/V data file is reproduced by CD-ROM etc., or is sold and distributed through a network.
[0003] This A/V data file is treated with a personal computer. And a user can reproduce and enjoy this A/V data file with the display unit and audio equipment which were connected to this personal computer.
[0004]
[Problem(s) to be Solved by the Invention] By the way, the record medium with which the video signal also conventionally digitized in the so-called A/V device and the sound signal were recorded was treated. In the A/V device, as it was called only playback or record, and playback, for example, the function to the A/V data treated was limited. Therefore, the device in which copyright is protected comparatively easily was realizable by adding the information about copyright to the A/V data recorded on the record medium to the A/V data treated in such an A/V device.
[0005] however, the A/V data treated in this A/V device to the above A/V data files — the device in which copyright was protected was not introduced like. Therefore, a copy and processing of this A/V data file will be performed freely, and there was a trouble that infringement of copyright will overrun.
[0006] Therefore, the purpose of this invention gives copyright information to the A/V data file treated on a computer, and is to offer the protection-of-copyrights approach of digital data and a protection system which protect the copyright of this A/V data file based on this information.

[0007]
[Means for Solving the Problem] In the protection-of-copyrights approach of the digital data created in order that this invention might solve the technical problem mentioned above The step of the encryption which enciphers copyright information based on an encryption key, and the step of copyright information storing which stores the enciphered copyright information in the predetermined field of a file, It is the protection-of-copyrights approach of the digital data which accesses to a file and is characterized by having the step of the decryption which decrypts the enciphered copyright information, and the step of the protection of copyrights which performs protection of copyrights based on the decrypted copyright information.
[0008] Moreover, this invention is set to the copyright protection system of the created digital data, in order to solve the technical problem mentioned above. An encryption means to

encipher copyright information based on an encryption key, and a copyright information storing means to store the enciphered copyright information in the predetermined field of a file, It is the copyright protection system of the digital data which accesses to a file and is characterized by having a decryption means to decrypt the enciphered copyright information, and the copyright safeguard which performs protection of copyrights based on the decrypted copyright information.

[0009] As mentioned above, since the enciphered copyright information which was stored in the predetermined field of a file is decrypted and protection of copyrights is made based on this decrypted copyright information, rewriting of the unjust copyright information by a user etc. is carried out by the ability not doing, and this invention can protect the copyright of data more certainly.

[0010]

[Embodiment of the Invention] Hereafter, one gestalt of implementation of this invention is explained. In this invention, copyright information is given as attribute (property) information in the A/V data file treated on a computer. Since this copyright information is enciphered and written in, it is protected from rewriting by a user's editor etc. This enciphered copyright information is referred to in case data are read from this A/V data file.

[0011] Drawing 1 shows roughly the system configuration assumed in the following explanation. Here, the computers 3a and 3b of the side which receives the above-mentioned computer 1 and above-mentioned A/V data file of an A/V data file sending area to the predetermined network 2, and the system to which ... is connected are assumed in this way. In addition, two or more connection also of the computer 1 of a sending area can be made like a reception side. Moreover, these computers 1 and 3a and 3b, and ... operate on predetermined OS (Operation System). Although mentioned later for details, this OS has a function corresponding to the copyright protection system in one gestalt of this operation.

[0012] By computer 1 of a sending area, the A/V data file created with the predetermined application software A (Software A is called hereafter) is received by the computers 3a and 3b by the side of reception, and ... through a network 2. And, for example in computer 3a, this A/V data file is read using the predetermined application software B (Software B is called hereafter). In addition, you may be Software A and the same application software as Software B.

[0013] An above-mentioned configuration is an example, and this invention can be applied also when the personal computer and digital video tape recorder which contained for example, the DVD(Digital Versatile Disk)-ROM drive are connected.

[0014] Drawing 2 shows roughly an example of the A/V data file structure in one gestalt of this operation. Data have a file structure general on the whole, and consist of a header unit, data division, and the delimiter section.

[0015] A header unit is a field which the attribute (property) information on this data file describes. This property information consists of information, such as information required in order that software and OS may identify this file, for example, the file name of this file, file format, and data size. Furthermore, in this one gestalt, the copyright information enciphered by this property information is included. This copyright information is read by OS or Software A and B, and the protection of copyrights to this file is made based on this copyright information. Since the copyright information for protection of copyrights is stored as property information on a file, this copyright information cannot be deleted.

[0016] The body of A/V data, i.e., voice data, and image data are stored in data division. Not only the body of A/V data but a program, a script, etc. may be stored in these data division. Moreover, these A/V data, a program, etc. can be made intermingled, and it can also store. In the delimiter section, the termination information on this file describes, for example.

[0017] Above-mentioned copyright information consists of information (APS (Analog Protection System) is called) which directs the copy limit system to the control information (CGMS (Copy Generation Management System) is called) and the analog video signal about a limit of a copy generation in this invention. You may make it include information required since authors, such as an author name of the data stored, for example and the creation date, assert the copyright of that data the data division of this A/V data file, or besides such information and the information which performs discernment of an author, for example, a personal identification

number, and ID in this copyright information.
[0018] An example of CGMS information and APS information is shown in drawing 3 . As shown in this drawing 3 A, CGMS information consists of 2-bit data, for example, is defined as follows. [0019] 00: It is 11:copy failure [0020] which can be possible 01:intact 10:copied [ one-generation ] in a copy. It is judged by reading and referring to this CGMS information by OS and software with which this A/V data file is involved whether it is possible to save this file.
[0021] Drawing 4 shows the flow chart of the copy generation limit by CGMS. When it is going to copy a file including CGMS information, for example, first, the header unit of a file is read and the CGMS information included in copyright information is extracted. And in the following step S2, it is judged whether this CGMS information is in which condition of the above-mentioned definitions. If CGMS information is '00', processing will shift to step S5. And in step S5, it is carried out [ that this file can be saved and ] according to a definition, a copy is performed, and a file is saved.
[0022] Moreover, if CGMS information is '11' which does not permit the copy of a file, processing will shift to step S3 and a file will be made impossible [ preservation ] according to a commuter's ticket.
[0023] If CGMS information is '10' which permits the copy of only one generation of a file, processing will further shift to step S4. CGMS information is changed into '11' which does not permit the copy of a file from '10' in step S4. When CGMS information is changed, processing shifts to step S5, a copy is performed, and a file is saved. Since CGMS information is changed into '11', this file is made impossible [ a copy ] and, thereby, a generation limit of a copy is made.
[0024] In addition, in fact, the contents of the file are once read into buffer memory etc., and the copy of a file is made by being written in another field of data carriers, such as memory and a disk. Therefore, the copy of this file can be treated on a par with preservation of a file.
[0025] Moreover, as shown in drawing 3 B, APS information consists of 2-bit data like above-mentioned CGMS information, for example, is defined as follows.
[0026] 00: APS OFF01 :P SP ON, split burst OFF 10 :P SP ON, two-line split burst ON 11 :P SP ON, four-line split burst ON [0027] This APS information is a predetermined approach, is superimposed by the analog video signal, for example, is sent out to an external video tape recorder and an external television monitor. When these equipments that received this APS information support this APS, record and projecting of this video signal can be blocked with the signal for anti-copying generated based on the signal for an analog copy limit generated according to the definition.
[0028] APS The signal for an analog copy limit is not generated in OFF. PSP ON means operating the system which superimposes the signal for anti-copying containing a false synchronizing signal to an analog video signal. In operating this system, AGC of a video tape recorder to which this video signal was supplied is made to malfunction, and record of a normal image can be blocked.
[0029] Moreover, ON of a split burst means operating the system which adds the color burst signal which inserted the reversal burst signal to the part to an analog video signal. In operating this system, with a monitor, a video tape recorder, etc. to which this video signal was supplied, APC cannot carry out normal actuation but can block projecting of a normal image. As a split burst, two methods of the two-line split burst which adds a reversal burst signal per two lines, and the four-line split burst which adds a reversal burst signal per four lines are prepared, and it is made as [ operate / one of these / alternatively ].
[0030] Drawing 5 shows roughly transition of processing between the software A and OS11 and the A/V data files 12 at the time of saving an A/V data file. The A/V data file 12 exists on memory (not shown) at the beginning, and is saved from this memory to record media (not shown), such as a hard disk, by directing preservation of this file 12 to Software A. In addition, this is applicable to preservation of the A/V data which were not restricted to this example, for example, were transmitted through the copy of the A/V data file from the 1st field to the 2nd field of a hard disk, or the network etc.
[0031] In the computer shown in this example, access to various devices by software, such as memory and a hard disk, is altogether made through OS11. Preservation of the created A/V

data file 12 is directed to Software A. These directions are predetermined formats, with are transmitted from Software A to OS11. And the key kc which Software A has is passed to OS11. Then, the copyright information on the A/V data file 12 which exists on memory is first read by OS11. Although mentioned later, since it is enciphered, this copyright information is a predetermined approach, with is decrypted.

[0032] CGMS information is extracted from the decoded copyright information, and it is judged according to the flow chart shown in above-mentioned drawing 4 whether this A/V data file 12 can be saved. When judged [ that it can save and ] as a result of this decision, this A/V data file 12 is written in and saved to the predetermined field of a hard disk. And by OS11, the write-in check of this file 12 is made, confirmed information is transmitted to Software A, and it is supposed in the software A which received this information that preservation of a file 12 was completed correctly.

[0033] The copyright information included in a header unit has a possibility that it may be easily rewritten by the user using the editor which can edit binary data. Then, in this invention, as mentioned above, this copyright information is enciphered by the predetermined approach. Drawing 6 shows an example of the approach of encryption of this copyright information roughly. For example, copyright information is created with creation of the A/V data in the above-mentioned software A. Information required since copyrights of the A/V data stored in this file, such as for example, an author name and a data origination day, are asserted, and above-mentioned CGMS information are included in this copyright information.

[0034] This copyright information is enciphered based on the encryption key kc which consists of a predetermined character string. The encryption key kc is generated based on a user's password Pw entered to the software B which reads the software A which creates an above-mentioned A/V data file, and the created file depending on specific software, and is reproduced or performed. Moreover, it is good though such software has this key kc beforehand.

[0035] The approach of performing by repeating character transposition and substitution to the notation or character string which is a predetermined approach based on Key kc as an example of encryption with this key kc, with constitutes copyright information is mentioned. While the enciphered copyright information is stored in a header unit as property information, the created A/V data are stored in data division, and an A/V data file is created.

[0036] As roughly shown in drawing 7 , the enciphered copyright information which is included in this A/V data file is Key kc, with is decrypted in a procedure contrary to the time of encryption. That is, the property information stored in the header unit of an A/V data file in Software B is read, and the enciphered copyright information which is included in this property information is extracted, for example. And the key kc which Software B has beforehand is used, and the copyright information which is a predetermined approach, with was enciphered based on Key kc is decrypted. The copy generation limit by above-mentioned CGMS is made to this decrypted copyright information.

[0037] In addition, the procedure of encryption/decryption of the copyright information shown in these drawing 6 and drawing 7 is theoretic, and it does not stop at being applied to one gestalt of this operation, but is applied also to the modification mentioned later.

[0038] Drawing 8 fits the procedure of encryption of the copyright information shown in above-mentioned drawing 6 and above-mentioned drawing 7 , and a decryption to one gestalt of this operation, and shows it more concretely. In this example, the encryption key kc at the time of enciphering copyright information is generated in OS11 based on the user password Pw and the master key km.

[0039] The user password Pw consists of a predetermined character string specified by the user, and is set up according to an individual in OS11 to the user who logs in. Moreover, this password Pw may be made to be set up in Software A. When Password Pw is set up in OS11 and it is set up in every starting of OS11, and Software A, a user is asked for an input for every starting of Software A. The master key km is set up by the user registration which consists of a predetermined character string, for example, is made in the case of install to the computer 1 of OS11.

[0040] The copyright information enciphered from the property information on the header unit of the A/V data file 12 is read by OS11. This copyright information is decrypted in OS11 based

on the above-mentioned key kc. And CGMS information is extracted from the decrypted copyright information, and prohibition/authorization of preservation of this file 12 are judged based on this CGMS information.
[0041] In this case, based on the decrypted copyright information, prohibition/authorization of the access [ itself ] to this file 12 can be judged. This copyright information is passed to Software A, Password Pw and this copyright information are collated in Software A, and this is made by passing that result to OS11, when Password Pw is set up to Software A.
[0042] In case CGMS information is set up on the other hand to the A/V data created in Software A and it is saved as an A/V data file, in OS11, encryption of copyright information is made based on Key kc.
[0043] With one gestalt of this operation, processing called collating and rewriting of CGMS information for the protection of copyrights of an A/V data file is made in OS11. On this OS11, copyright information is set up to all the files created, and in case it is all file manipulation, processing of collating of this set-up copyright information etc. is made. Then, it is necessary to give compatibility to the file manipulation which does not support this copyright protection system and which was created on other OS's.
[0044] Drawing 9 shows the flow chart of access to the file in consideration of the compatibility of this file in OS11. If access to a file is made, in step S10, it will be judged first whether this file supports the copyright protection system by OS11. This decision can describe the flag which shows that to a header unit at the file which supports the copyright protection system in OS11, and can be performed by investigating the existence of this flag. Moreover, you may make it investigate the existence of the copyright information of a header unit itself.
[0045] If it is judged that a copyright protection system is not supported, the means of protection of copyrights against this file will not be taken, but preservation of a file will be made in step S17.
[0046] On the other hand, if it is judged that the file supports the copyright protection system at step S10, processing will shift to step S11. And the copyright information on this file is read and decrypted in step S11. The encryption key kc is required from predetermined software (for example, above-mentioned software A and B) from OS11, and this decryption is made based on the key kc passed from that software to this demand. If a decryption of copyright information is made, processing will shift to step S12.
[0047] At step S12, CGMS information is extracted from the decrypted copyright information. And the condition of CGMS information is judged at the following step S13. If it is CGMS='11', processing will shift to step S14 and file preservation will be made improper according to the definition of above-mentioned CGMS. Moreover, if it is CGMS='00', since file preservation will be enabled according to a definition, processing shifts to step S16. If it is CGMS='10', processing will shift to step S15 and CGMS information will further be rewritten by '11'. And processing shifts to the following step S16.
[0048] Copyright information is enciphered in step S16. The encryption key kc is required from predetermined software from OS11, and this encryption is made based on the key kc passed from that software to this demand. If encryption is made, let copyright information included in the header unit of a file be the copyright information enciphered at this step S16. And this file is saved at the following step S17.
[0049] In addition, although [ above-mentioned explanation / each of the computer 1 connected to the network 2 and 3a and 3b, and ... ] same OS11 is carried altogether, this is not limited to this example. If it is a common protocol mutually, with data communication can be performed even when an OS which is different to a computer 1 and 3a and 3b, and .... respectively is carried, the copyright protection system by this invention is applicable.
[0050] Moreover, an above-mentioned flow chart can set up alternatively the file for which protection of copyrights is not needed by applying this processing, although the compatibility of the file which does not support a copyright protection system was taken into consideration.
[0051] This file being reproduced or performed by the computer, and an A/V data file being made into the video signal of an analog form or a digital method by it the copy as a data file not only being performed, but, and being outputted outside is also considered. This outputted video signal is recorded for example, by the analog video tape recorder, and, thereby, the infringement

of copyright to A/V data may produce it. Therefore, it is necessary to take into consideration also about the protection of copyrights in such a case.
[0052] Drawing 10 shows notionally the approach of data conversion in case the A/V data reproduced from the A/V data file are outputted to the computer exterior. Here, the example by which A/V data are changed and outputted to the analog RGB signal is shown. It does not illustrate, but by Software A, the A/V data file 12 is reproduced and A/V data are outputted also for **. This A/V data is made into the component video signal which both becomes that D/A conversion supplied and carried out to an encoder 20 from the signal of each color of RGB. R signal is supplied to one input edge of an adder 22 among this component video signal.
[0053] Synchronizing with a video signal, this adder 22 is predetermined timing, with can control the addition to the video signal supplied to one input edge of the signal supplied to the input edge of another side. This is made in an encoder 20 by supplying the control signal generated based on the timing signal used when changing A/V data into a video signal to this adder 22.
[0054] On the other hand, copyright information is read from an A/V data file by software OS [ A and ] 11. This copyright information is decrypted with Key kc, and APS information is extracted. And the signal for an analog copy limit is generated based on this APS information, and this generated signal is supplied to the input edge of another side of an adder 22. In an adder 22, this signal is added to the horizontal or perpendicular blanking period of R signal currently supplied by one input edge.
[0055] Although not illustrated, this analog video signal is supplied, for example to the RGB code / composite video signal converter corresponding to APS while supplying and projecting it to a monitor. Since the signal for a copy limit is superimposed at the blanking period, there is no direct effect in projecting to a monitor. However, when it is outputted outside as a composite video signal through the RGB code / composite video signal transducer corresponding to APS, the signal for anti-copying based on the definition of APS information with which an example is shown is superimposed or added to above-mentioned drawing 3 B to this video signal. Therefore, even if it records this video signal on a video tape etc., it cannot reproduce as a normal image but the copyright over A/V data can be protected as a result.
[0056] In addition, when an A/V data file is reproduced and it is outputted outside as digital image data, the CGMS information and APS information which were extracted from copyright information are transmitted as it is, for example, it is recorded on the predetermined field of a tape by the digital video cassette recorder. Therefore, anti-copying effectiveness can be acquired easily even in this case.
[0057] Next, the modification of one gestalt of implementation of this invention is explained. Drawing 11 shows roughly an example of the A/V data file structure in this modification. In this modification, the A/V data stored in data division are enciphered based on the predetermined encryption key kd, and this key kd is enciphered with the copyright information on the header unit of an A/V data file based on a predetermined encryption key. In this modification, the protection of copyrights of A/V data is more firmly performed by enciphering the A/V data itself in this way.
[0058] Drawing 12 shows roughly an example of the approach of encryption of the A/V data file by this modification. In this example, encryption of copyright information and the data encryption key kd is performed using the customer management key ku distributed from an A/V data file supply side to a user.
[0059] A/V data are enciphered based on the data encryption key kd which is the supply side of this data and has been managed. It is made by this encryption by repeating character transposition and substitution according to the predetermined regulation based on Key kd. This enciphered A/V data is stored in the data division of an A/V data file. Moreover, the key kd used for this A/V data encryption is enciphered based on the customer management key ku managed with copyright information at the supply side of A/V data. This customer management key ku is set up to each of the customer who received supply of this A/V data, for example, and is passed from an A/V data supply side. In this way, in the copyright information and Key kd which were enciphered, it is stored in the header unit of an A/V data file as property information.
[0060] Drawing 13 shows roughly an example of the approach of a decryption of the A/V data

file by this modification. In the A/V data file passed to the user, a header unit is read from the supply side of A/V data, and the copyright information and the data encryption key kd which were enciphered are extracted from it. Moreover, the customer management key ku is beforehand passed from an A/V data supply side to a user. The copyright information and Key kd which were extracted from the header unit and which were enciphered are decrypted with this customer management key ku. And the enciphered A/V data which were stored in data division are decrypted with this decrypted customer management key ku.

[0061] Like this example, by using the customer management key ku, an A/V data supply side can limit use of an A/V data file to a user, and can perform customer management by the side of A/V data supply. Therefore, the approach using this customer management key ku is used to the A/V data file mass-produced, for example, and is suitable.

[0062] The approach of protection of copyrights [ in / on the other hand / one gestalt of above-mentioned operation ] uses to protection of the copyright about creation of an individual and is suitable.

[0063] In addition, not only this example but this modification can use the encryption key kc used instead of the customer management key ku in one gestalt of above-mentioned operation. Of course in this case, customer management by the A/V data supply side is not performed strictly.

[0064] In one gestalt of above-mentioned operation, and its modification, although it explained that this invention was applied to OS corresponding to copyright information processing, this is not limited to this example. drawing 14 — this — invention — being another — a modification — — ****** — copyright — information processing — corresponding — **** — OS — receiving — this — invention — applying — having had — the time — software — A — ' — OS — 11 — — ' — A/V — a data file — 12 — between — it can set — processing — transition — rough — — being shown . In addition, this another modification is applicable also to the file structure of what [ by one gestalt of above-mentioned operation, and its modification ] one.

[0065] In this another modification, read-out of the copyright information from the A/V data file currently made in OS11 and read decode of copyright information are performed on software A' in one gestalt of above-mentioned operation, and its modification. The A/V data file 12 exists on the memory which is not illustrated at the beginning, and is saved from this memory to the hard disk which is not illustrated, for example by directing preservation of this file 12 to software A'. In addition, this is applicable to preservation of the A/V data which were not restricted to this example, for example, were transmitted through the copy of the A/V data file from the 1st field to the 2nd field of a hard disk, or the network etc.

[0066] Preservation of the created A/V data file 12 is directed to software A'. Based on these directions, the header unit of the A/V data file 12 to property information is read, and copyright information is extracted from this read property information. This copyright information is enciphered with the encryption key kc which software A' has in the proper. Copyright information is decrypted and decoded based on this key kc.

[0067] In addition, the encryption key used for encryption of copyright information is not restricted to an encryption key kc like this example. For example, the customer management key ku passed to an A/V data file supply side to the above-mentioned user can be used as this encryption key.

[0068] CGMS information is extracted from the decoded copyright information, and it is judged according to the flow chart shown in above-mentioned drawing 4 whether this A/V data file 12 can be saved. When judged [ that it can save and ] as a result of this decision, this A/V data file 12 is written in and saved by OS11' to the predetermined field of a hard disk. And the write-in check of this file 12 is made by OS11', confirmed information is transmitted to software A', and it is supposed in software A' which received this information that preservation of a file 12 was completed correctly.

[0069]

[Effect of the Invention] As explained above, according to this invention, the copyright information for performing protection of copyrights is included in the property information on an A/V data file. Therefore, also to the A/V data treated on a computer, the device of protection of copyrights can be introduced and it is effective in infringement of copyright being prevented.

[0070] Moreover, according to this invention, the CGMS information which controls a generation limit of a copy to copyright information is included, and the protection of copyrights of A/V data is performed with the same concept as what is already introduced by the digital A/V device etc. Therefore, the effectiveness that adjustment can be taken is in the view of protection of copyrights between the A/V data on a computer, and a digital A/V device.
[0071] Furthermore, according to this invention, since it is enciphered, copyright information is protected from unjust rewriting by the user etc., and is effective in safety being high.
[0072] Since the property information in which copyright information is included in OS in the case of renewal of a file or preservation is referred to further again according to this invention, it is effective in the certainty of protection of copyrights increasing more compared with the case where same processing is performed, only with application software.
[0073] Moreover, since processing for the protection of copyrights by this invention is performed only by handling at most several bytes of data on software or OS, the newly because of protection of copyrights generated cost has the effectiveness which can be disregarded of being the thing of extent.
[0074] Furthermore, since the copyright information by this invention is treated as property information on an A/V data file, it cannot be deleted from a file but is effective in the ability to perform protection of copyrights more certainly.
[0075] Moreover, the copyright information by this invention is set up based on the protection of copyrights in the digital A/V device which already exists, and a common idea. Therefore, the A/V data based on this invention are effective in the ability to transmit as it is on an interface with a digital A/V device.

---

[Translation done.]

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing showing roughly the system configuration assumed in explanation.
[Drawing 2] It is drawing showing roughly an example of the A/V data file structure in one gestalt of operation.
[Drawing 3] It is the abbreviation diagram showing an example of CGMS information and APS information.
[Drawing 4] It is the flow chart of the copy generation limit by CGMS.
[Drawing 5] It is drawing showing roughly transition of processing between the software, OS's, and the A/V data files at the time of saving an A/V data file.
[Drawing 6] It is drawing showing an example of the approach of encryption of copyright information roughly.
[Drawing 7] It is drawing showing an example of a decryption of copyright information roughly.
[Drawing 8] It is drawing showing the procedure of encryption of copyright information, and a decryption more concretely.
[Drawing 9] It is the flow chart of access to the file in consideration of the compatibility of a file in OS.
[Drawing 10] It is drawing showing notionally the approach of data conversion in the case of carrying out the external output of the A/V data file.
[Drawing 11] It is drawing showing roughly an example of the A/V data file structure in a modification.
[Drawing 12] It is drawing showing roughly an example of the approach of the encryption of an A/V data file at the time of using the customer management key ku.
[Drawing 13] It is drawing showing roughly an example of the approach of the decryption of an A/V data file at the time of using the customer management key ku.
[Drawing 14] Transition of processing between software when OS does not support copyright information processing, OS, and an A/V data file is shown roughly.
[Description of Notations]
1, 3a, 3b [ ... Application software kc / ... An encryption key, kd / ... A data encryption key, km / ... A master key, ku / ... A customer management key Pw / ... User password ] ... A computer, 11 ... OS, 12 ... An A/V data file, A, B

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

---

CORRECTION OR AMENDMENT

---

[Kind of official gazette] Printing of amendment by the convention of 2 of Article 17 of Patent Law
[Section partition] The 3rd partition of the 7th section
[Publication date] June 7, Heisei 14 (2002. 6.7)

[Publication No.] JP,10-108148,A
[Date of Publication] April 24, Heisei 10 (1998. 4.24)
[Annual volume number] Open patent official report 10-1082
[Application number] Japanese Patent Application No. 8-277130
[The 7th edition of International Patent Classification]

H04N 7/08
7/081
G06F 15/00 330
G09C 1/00 660
H04N 7/167

[FI]

H04N 7/08 Z
G06F 15/00 330 Z
G09C 1/00 660 D
H04N 7/167 Z

[Procedure revision]
[Filing Date] March 14, Heisei 14 (2002. 3.14)
[Procedure amendment 1]
[Document to be Amended] Specification
[Item(s) to be Amended] Claim
[Method of Amendment] Modification
[Proposed Amendment]
[Claim(s)]
[Claim 1] In the protection-of-copyrights approach of the created digital data,
The step of the encryption which enciphers copyright information based on an encryption key,
The step of copyright information storing which stores in the predetermined field of a file the copyright information by which encryption was carried out [ above-mentioned ],
The step of the decryption which accesses to the above-mentioned file and decrypts the copyright information by which encryption was carried out [ above-mentioned ],
The step of the protection of copyrights which performs protection of copyrights based on the copyright information by which the decryption was carried out [ above-mentioned ]
The protection-of-copyrights approach of the digital data characterized by ****(ing).
[Claim 2] In the protection-of-copyrights approach of digital data according to claim 1,
The above-mentioned predetermined field is the protection-of-copyrights approach of the digital data characterized by being the field which stores the attribute information on the

above-mentioned file.
[Claim 3] In the protection-of-copyrights approach of digital data according to claim 1,
The step of other encryption which enciphers the body of data of the above-mentioned file stored in the above-mentioned file based on other encryption keys,
The step of other decryptions which decrypt the above-mentioned body of data based on an encryption key besides the above
It has in a pan.
The step of the above-mentioned encryption is the protection-of-copyrights approach of the digital data characterized by enciphering the above-mentioned copyright information, and an encryption key besides the above with the above-mentioned encryption key.
[Claim 4] In the copyright protection system of the created digital data,
An encryption means to encipher copyright information based on an encryption key,
A copyright information storing means to store in the predetermined field of a file the copyright information by which encryption was carried out [ above-mentioned ],
A decryption means to access to the above-mentioned file and to decrypt the copyright information by which encryption was carried out [ above-mentioned ],
The copyright protection system of the digital data characterized by having the copyright safeguard which performs protection of copyrights based on the copyright information by which the decryption was carried out [ above-mentioned ].

---

[Translation done.]

SCHOPPE, ZIMMERMANN, STÖCKELER & ZINKLER

PATENTANWÄLTE

European Patent Attorneys
European Trademark Attorneys

Patentanwälte · Postfach 246 · 82043 Pullach bei München

Fritz Schoppe*, Dipl.-Ing.
Tankred Zimmermann*, Dipl.-Ing.
Ferdinand Stöckeler*, Dipl.-Ing.
Franz Zinkler*, Dipl.-Ing.
Markus Schenk*, Dipl.-Phys.
Günter Hersina*, Dipl.-Ing.

Telefon/Telephone 089/790445-0
Telefax/Facsimile 089/7 90 22 15
Telefax/Facsimile 089/74996977
e-mail: szsz_iplaw@t-online.de

Glenn Patent Group
Attn.: Mr. Michael A. Glenn
3475 Edison Way, Suite L
Menlo Park, CA 94025
U.S.A.

March 10, 2005

**Telefax: 001-650-474-8401**

**US Patent Application Serial No. 09/913,690**
**Applicants: Niels RUMP; Jürgen KOLLER; Dr. Karlheinz BRANDENBURG;**
**Title: METHOD AND DEVICE FOR GENERATING A DATA STREAM AND METHOD AND DEVICE FOR PLAYING BACK A DATA STREAM**
**Your Ref.: SCHO0094**
**Our Ref.: FH991203PUS / mb**

Dear Michael:

Please be informed that we received in the parallel Japanese Patent Application an Office Action with the enclosed following Japanese prior art references:

- JP 10-108148
- JP 10-107787

I would like to ask you to please file an Information Disclosure Statement with the USPTO no later than March 17, 2005.

Thank you in advance.

Very truly yours,

i.V. Franz Zinkler

**Enc.:**
2 prior art references (by facsimile and airmail)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開平10－108148
(43)公開日　平成10年(1998)４月24日

| (51)Int.Cl.⁶ | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| H04N | 7/08 | | H04N | 7/08 | Z |
| | 7/081 | | G06F | 15/00 | 330Z |
| G06F | 15/00 | 330 | G09C | 1/00 | 660D |
| G09C | 1/00 | 660 | H04N | 7/167 | Z |
| H04N | 7/167 | | | | |

審査請求　未請求　請求項の数20　ＦＤ　(全 14 頁)

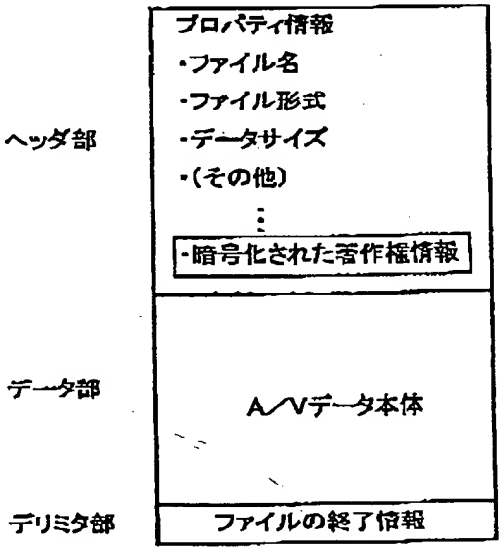
(21)出願番号　特願平8－277130

(22)出願日　平成８年(1996)９月27日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　鄧　照彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　弁理士　杉浦　正知

(54)【発明の名称】　ディジタルデータの著作権保護方法および保護システム

(57)【要約】
【課題】　コンピュータ上で扱われるＡ／Ｖデータファイルに対して著作権情報を持たせ、Ａ／Ｖデータの著作権を保護する。
【解決手段】　ファイルのヘッダ部に、ファイルのプロパティ情報として著作権情報が格納される。この著作権情報は、ファイルのコピーの世代制限情報からなり、所定の暗号化鍵ｋｃによって暗号化される。このファイルに対してアクセスした場合には、先ず、このヘッダ部から著作権情報が抽出される。アクセスを行なったユーザが暗号化鍵ｋｃを有していなければ著作権情報を復号化できないために、ファイルに格納されたＡ／Ｖデータを読み出すことができない。ファイルのコピーの際には、世代制限情報が書き換えられ再び著作権情報として格納されるため、コピーの世代を制限することができる。Ａ／Ｖデータ本体を別の暗号化鍵ｋｄで暗号化し、鍵ｋｄを著作権情報と共に鍵ｋｃで暗号化することによって、さらに確実に著作権保護を行なうことができる。



【特許請求の範囲】

【請求項１】　作成されたディジタルデータの著作権保護方法において、

著作権情報を暗号化鍵に基づき暗号化する暗号化のステップと、

上記暗号化された著作権情報をファイルの所定の領域に格納する著作権情報格納のステップと、

上記ファイルに対してアクセスし、上記暗号化された著作権情報を復号化する復号化のステップと、

上記復号化された著作権情報に基づき著作権保護を行なう著作権保護のステップとを有することを特徴とするディジタルデータの著作権保護方法。

【請求項２】　請求項１に記載のディジタルデータの著作権保護方法において、

上記所定の領域は、上記ファイルの属性情報を格納する領域であることを特徴とするディジタルデータの著作権保護方法。

【請求項３】　請求項１に記載のディジタルデータの著作権保護方法において、

上記著作権情報は、上記ファイルのコピー世代を制限する情報からなることを特徴とするディジタルデータの著作権保護方法。

【請求項４】　請求項１に記載のディジタルデータの著作権保護方法において、

上記著作権情報は、上記ファイルに対して所定のファイル操作を行なっても保存されることを特徴とするディジタルデータの著作権保護方法。

【請求項５】　請求項１に記載のディジタルデータの著作権保護方法において、

上記暗号化のステップ、上記著作権情報格納のステップ、上記復号化のステップ、および上記著作権保護のステップのそれぞれは、所定のアプリケーションソフトウェア上でなされることを特徴とするディジタルデータの著作権保護方法。

【請求項６】　請求項１に記載のディジタルデータの著作権保護方法において、

上記暗号化のステップ、上記著作権情報格納のステップ、上記復号化のステップ、および上記著作権保護のステップのそれぞれは、オペレーションシステム上でなされることを特徴とするディジタルデータの著作権保護方法。

【請求項７】　請求項１に記載のディジタルデータの著作権保護方法において、

上記ファイルに対して所定のファイル操作をすることによって得られたディジタルＡ／Ｖデータを他の形式の信号に変換し伝送する際には、上記著作権情報は、上記他の形式に対応する形式に変換されて、上記他の形式の信号と共に上記伝送されることを特徴とするディジタルデータの著作権保護方法。

【請求項８】　請求項１に記載のディジタルデータの著作権保護方法において、



上記ファイルに格納される上記ファイルのデータ本体を他の暗号化鍵に基づき暗号化する他の暗号化のステップと、

上記データ本体を上記他の暗号化鍵に基づき復号化する他の復号化のステップとをさらに有し、

上記暗号化のステップは、上記著作権情報と上記他の暗号化鍵とを上記暗号化鍵で暗号化することを特徴とするディジタルデータの著作権保護方法。

【請求項９】　請求項８に記載のディジタルデータの著作権保護方法において、

上記他の暗号化のステップおよび上記他の復号化のステップのそれぞれは、所定のアプリケーションソフトウェア上でなされることを特徴とするディジタルデータの著作権保護方法。

【請求項１０】　請求項８に記載のディジタルデータの著作権保護方法において、

上記他の暗号化のステップおよび上記他の復号化のステップのそれぞれは、オペレーションシステム上でなされることを特徴とするディジタルデータの著作権保護方法。

【請求項１１】　作成されたディジタルデータの著作権保護システムにおいて、

著作権情報を暗号化鍵に基づき暗号化する暗号化手段と、

上記暗号化された著作権情報をファイルの所定の領域に格納する著作権情報格納手段と、

上記ファイルに対してアクセスし、上記暗号化された著作権情報を復号化する復号化手段と、

上記復号化された著作権情報に基づき著作権保護を行なう著作権保護手段とを有することを特徴とするディジタルデータの著作権保護システム。

【請求項１２】　請求項１１に記載のディジタルデータの著作権保護システムにおいて、

上記所定の領域は、上記ファイルの属性情報を格納する領域であることを特徴とするディジタルデータの著作権保護システム。

【請求項１３】　請求項１１に記載のディジタルデータの著作権保護システムにおいて、

上記著作権情報は、上記ファイルのコピー世代を制限する情報からなることを特徴とするディジタルデータの著作権保護システム。

【請求項１４】　請求項１１に記載のディジタルデータの著作権保護システムにおいて、

上記著作権情報は、上記ファイルに対して所定のファイル操作を行なっても保存されることを特徴とするディジタルデータの著作権保護システム。

【請求項１５】　請求項１１に記載のディジタルデータの著作権保護システムにおいて、

上記暗号化手段、上記著作権情報格納手段、上記復号化

手段、および上記著作権保護手段のそれぞれは、所定のアプリケーションソフトウェアが有することを特徴とするディジタルデータの著作権保護システム。

【請求項16】　請求項11に記載のディジタルデータの著作権保護システムにおいて、
上記暗号化手段、上記著作権情報格納手段、上記復号化手段、および上記著作権保護手段のそれぞれは、オペレーションシステムが有することを特徴とするディジタルデータの著作権保護システム。

【請求項17】　請求項11に記載のディジタルデータの著作権保護システムにおいて、
上記ファイルに対して所定のファイル操作をすることによって得られたディジタルA／Vデータを他の形式の信号に変換し伝送する際には、上記著作権情報は、上記他の形式に対応する形式に変換されて、上記他の形式の信号と共に上記伝送されることを特徴とするディジタルデータの著作権保護システム。

【請求項18】　請求項11に記載のディジタルデータの著作権保護システムにおいて、
上記ファイルに格納される上記ファイルのデータ本体を他の暗号化鍵に基づき暗号化する他の暗号化手段と、
上記データ本体を上記他の暗号化鍵に基づき復号化する他の復号化手段とをさらに有し、
上記暗号化手段は、上記著作権情報と上記他の暗号化鍵とを上記暗号化鍵で暗号化することを特徴とするディジタルデータの著作権保護システム。

【請求項19】　請求項18記載のディジタルデータの著作権保護システムにおいて、
上記他の暗号化手段および上記他の復号化手段のそれぞれは、所定のアプリケーションソフトウェアが有することを特徴とするディジタルデータの著作権保護システム。

【請求項20】　請求項18記載のディジタルデータの著作権保護システムにおいて、
上記他の暗号化手段および上記他の復号化手段のそれぞれは、オペレーションシステムが有することを特徴とするディジタルデータの著作権保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、データファイルの属性情報として著作権情報を持たせ、この著作権情報を所定の方法に基づき暗号化することで、著作物として作成されたディジタルデータの著作権を保護するようなディジタルデータの著作権保護方法および保護システムに関する。

【0002】

【従来の技術】近年、コンピュータの高速化やディジタル記録媒体の大容量化、コンピュータネットワークの発達、また、画像圧縮技術の発達などが目ざましい。それに伴い、ディジタル化された映像信号や音声信号、あるいはコンピュータによって作成されたCG(Computer Graphics)作品などがA／V(Audio/Video)データファイルとして記録されることが行なわれている。こうして記録されたA／Vデータファイルは、CD－ROMなどに複製され、あるいはネットワークを介して販売ならびに配布される。

【0003】このA／Vデータファイルは、例えばパーソナルコンピュータによって扱われる。そして、ユーザは、このパーソナルコンピュータに接続されたディスプレイ装置やオーディオ装置によってこのA／Vデータファイルを再生して楽しむことができる。

【0004】

【発明が解決しようとする課題】ところで、従来でも、所謂A／V機器において、ディジタル化された映像信号や音声信号が記録された記録媒体が扱われていた。A／V機器においては、例えば再生のみ、あるいは記録および再生のみといったように、扱われるA／Vデータに対する機能が限定されていた。したがって、このような、A／V機器において扱われるA／Vデータに対しては、記録媒体に記録されたA／Vデータに対して著作権に関する情報を付加することで、比較的容易に著作権の保護を行なう機構を実現することができた。

【0005】ところが、上述のようなA／Vデータファイルに対しては、このA／V機器において扱われるA／Vデータように、著作権の保護を行なう機構が導入されていなかった。そのため、このA／Vデータファイルの複写や加工が自由に行われてしまい、著作権の侵害が横行してしまうという問題点があった。

【0006】したがって、この発明の目的は、コンピュータ上で扱われるA／Vデータファイルに対して著作権情報を持たせ、この情報に基づきこのA／Vデータファイルの著作権を保護するようなディジタルデータの著作権保護方法および保護システムを提供することにある。

【0007】

【課題を解決するための手段】この発明は、上述した課題を解決するために、作成されたディジタルデータの著作権保護方法において、著作権情報を暗号化鍵に基づき暗号化する暗号化のステップと、暗号化された著作権情報をファイルの所定の領域に格納する著作権情報格納のステップと、ファイルに対してアクセスし、暗号化された著作権情報を復号化する復号化のステップと、復号化された著作権情報に基づき著作権保護を行なう著作権保護のステップとを有することを特徴とするディジタルデータの著作権保護方法である。

【0008】また、この発明は、上述した課題を解決するために、作成されたディジタルデータの著作権保護システムにおいて、著作権情報を暗号化鍵に基づき暗号化する暗号化手段と、暗号化された著作権情報をファイルの所定の領域に格納する著作権情報格納手段と、ファイルに対してアクセスし、暗号化された著作権情報を復号

化する復号化手段と、復号化された著作権情報に基づき著作権保護を行なう著作権保護手段とを有することを特徴とするディジタルデータの著作権保護システムである。

【０００９】上述したように、この発明は、ファイルの所定の領域に格納された、暗号化された著作権情報を復号化し、この復号化された著作権情報に基づいて著作権保護がなされるので、ユーザなどによる不正な著作権情報の書き換えができなくされ、データの著作権をより確実に保護することができる。

【００１０】

【発明の実施の形態】以下、この発明の実施の一形態について説明する。この発明では、コンピュータ上で扱われるＡ／Ｖデータファイルにおいて、属性（プロパティ）情報として著作権情報を持たせる。この著作権情報は、暗号化されて書き込まれるため、ユーザのエディタなどによる書き換えから保護される。この暗号化された著作権情報は、このＡ／Ｖデータファイルからデータが読み出される際に参照される。

【００１１】図１は、以下の説明において想定するシステム構成を概略的に示す。ここでは、このように、所定のネットワーク２に対して、上述のＡ／Ｖデータファイル送出側のコンピュータ１とＡ／Ｖデータファイルを受け取る側のコンピュータ３ａ，３ｂ，・・・とが接続されるシステムが想定される。なお、送出側のコンピュータ１も、受け取り側と同様に、複数接続されることができる。また、これらコンピュータ１および３ａ，３ｂ，・・・は、所定のＯＳ（Operation System）上で動作する。詳細は後述するが、このＯＳは、この実施の一形態における著作権保護システムに対応した機能を有する。

【００１２】送出側のコンピュータ１で、所定のアプリケーションソフトウェアＡ（以下、ソフトウェアＡと称する）で作成されたＡ／Ｖデータファイルがネットワーク２を介して受け取り側のコンピュータ３ａ，３ｂ，・・・に受け取られる。そして、例えばコンピュータ３ａにおいて、所定のアプリケーションソフトウェアＢ（以下、ソフトウェアＢと称する）を用いてこのＡ／Ｖデータファイルが読み出される。なお、ソフトウェアＡおよびソフトウェアＢとは、同一のアプリケーションソフトウェアであってもよい。

【００１３】上述の構成は一例であって、この発明は、例えばＤＶＤ（Digital Versatile Disk）－ＲＯＭドライブを内蔵したパーソナルコンピュータとディジタルＶＴＲとが接続されたような場合にも適用することができる。

【００１４】図２は、この実施の一形態におけるＡ／Ｖデータファイル構造の一例を概略的に示す。データは、全体的には一般的なファイル構造を有し、ヘッダ部，データ部，およびデリミタ部とからなる。

【００１５】ヘッダ部は、このデータファイルの属性



（プロパティ）情報が記される領域である。このプロパティ情報は、ソフトウェアやＯＳがこのファイルを識別するために必要な情報、例えばこのファイルのファイル名，ファイル形式，およびデータサイズなどの情報からなる。さらに、この一形態においては、このプロパティ情報に、暗号化された著作権情報が含まれる。ＯＳやソフトウェアＡあるいはＢによってこの著作権情報が読み込まれ、この著作権情報に基づきこのファイルに対する著作権保護がなされる。著作権保護のための著作権情報がファイルのプロパティ情報として格納されるため、この著作権情報は、削除することができない。

【００１６】データ部には、Ａ／Ｖデータ本体、すなわち、音声データおよび／または画像データが格納される。このデータ部には、Ａ／Ｖデータ本体に限らず、例えばプログラムやスクリプトなどを格納してもよい。また、これらＡ／Ｖデータおよびプログラムなどを混在させて格納することもできる。デリミタ部には、例えばこのファイルの終了情報が記される。

【００１７】この発明においては、上述の著作権情報は、コピー世代の制限に関する制御情報（ＣＧＭＳ（Copy Generation Management System）と称する）およびアナログビデオ信号に対するコピー制限システムを指示する情報（ＡＰＳ（Analog Protection System）と称する）とからなる。この著作権情報には、これらの情報の他にも、例えばこのＡ／Ｖデータファイルのデータ部に格納されるデータの著作者名，作成日などの、著作者がそのデータの著作権を主張するために必要な情報や、著作者の識別を行なう情報、例えば暗証番号やＩＤを含ませるようにしてもよい。

【００１８】ＣＧＭＳ情報およびＡＰＳ情報の一例を図３に示す。この図３Ａに示すように、ＣＧＭＳ情報は、２ビットのデータからなり、例えば下記のように定義される。

【００１９】００：コピー可能

０１：未使用

１０：コピー１世代可能

１１：コピー不可

【００２０】このＡ／Ｖデータファイルが係わるＯＳやソフトウェアによって、このＣＧＭＳ情報が読み出され参照されることによって、このファイルを保存することが可能であるかどうかが判断される。

【００２１】図４は、ＣＧＭＳによるコピー世代制限のフローチャートを示す。ＣＧＭＳ情報を含むファイルを例えばコピーしようとした場合、先ず、ファイルのヘッダ部が読み込まれ、著作権情報に含まれるＣＧＭＳ情報が抽出される。そして、次のステップＳ２において、このＣＧＭＳ情報が上述の定義のうちのどの状態であるかが判断される。若し、ＣＧＭＳ情報が‘００’であれば、処理はステップＳ５に移行する。そして、ステップＳ５において、定義に従いこのファイルが保存可能であ

るとされ、コピーが行なわれファイルが保存される。

【００２２】また若し、ＣＧＭＳ情報がファイルのコピーを許可しない‘１１’であれば、処理はステップＳ３に移行し、定期に従いファイルが保存不可とされる。

【００２３】さらに若し、ＣＧＭＳ情報がファイルの１世代のみのコピーを許可する‘１０’であれば、処理はステップＳ４に移行する。ステップＳ４では、ＣＧＭＳ情報が‘１０’からファイルのコピーを許可しない‘１１’に変更される。ＣＧＭＳ情報が変更されると、処理はステップＳ５に移行し、コピーが行なわれ、ファイルが保存される。ＣＧＭＳ情報が‘１１’に変更されているため、このファイルはコピー不可とされ、これによりコピーの世代制限がなされる。

【００２４】なお、実際には、ファイルのコピーは、例えばファイルの内容が一旦バッファメモリなどに読み込まれ、メモリやディスクなどのデータ記憶媒体の別の領域に書き込まれることによってなされる。したがって、このファイルのコピーは、ファイルの保存と同等に扱うことができる。

【００２５】また、図３Ｂに示すように、ＡＰＳ情報は、上述のＣＧＭＳ情報と同様に２ビットのデータからなり、例えば下記のように定義される。

【００２６】００：ＡＰＳ　ＯＦＦ
０１：ＰＳＰ　ＯＮ，スプリットバーストＯＦＦ
１０：ＰＳＰ　ＯＮ，２ラインスプリットバーストＯＮ
１１：ＰＳＰ　ＯＮ，４ラインスプリットバーストＯＮ

【００２７】このＡＰＳ情報は、所定の方法で以てアナログビデオ信号に重畳されて、例えば外部のビデオテープレコーダやテレビジョンモニタに送出される。このＡＰＳ情報を受け取ったこれらの装置がこのＡＰＳに対応している場合、定義に従い発生されたアナログコピー制限用信号に基づいて生成されたコピー防止用信号によって、このビデオ信号の記録や映出を妨害することができる。

【００２８】ＡＰＳ　ＯＦＦでは、アナログコピー制限用信号を発生しない。ＰＳＰ　ＯＮは、疑似同期信号を含むコピー防止用信号を、アナログビデオ信号に対して重畳するシステムを動作させることを意味する。このシステムを動作させることで、このビデオ信号を供給されたビデオテープレコーダのＡＧＣを誤動作させ、正常な画像の記録を妨害することができる。

【００２９】また、スプリットバーストのＯＮは、その一部に反転バースト信号を挿入したカラーバースト信号を、アナログビデオ信号に対して付加するシステムを動作させることを意味する。このシステムを動作させることで、このビデオ信号を供給されたモニタやビデオテープレコーダなどで、ＡＰＣが正常な動作をすることができず、正常な画像の映出を妨害することができる。スプリットバーストとしては、２ライン単位で反転バースト信号を付加する２ラインスプリットバーストと、４ライン単位で反転バースト信号を付加する４ラインスプリットバーストとの二つの方式が用意され，その一方を選択的に動作させるようになされている。

【００３０】図５は、Ａ／Ｖデータファイルを保存する際の、ソフトウェアＡ，ＯＳ１１，およびＡ／Ｖデータファイル１２間における処理の推移を概略的に示す。Ａ／Ｖデータファイル１２は、例えば当初メモリ（図示しない）上に存在し、ソフトウェアＡに対してこのファイル１２の保存を指示することによって、このメモリからハードディスクなどの記録媒体（図示しない）に対して保存される。なお、これはこの例に限られず、例えばハードディスクの第１の領域から第２の領域へのＡ／Ｖデータファイルのコピー、あるいはネットワークを介して伝送されたＡ／Ｖデータの保存などにも適用できる。

【００３１】この例に示されるコンピュータにおいて、ソフトウェアによるメモリやハードディスクなどの各種デバイスに対するアクセスは、全てＯＳ１１を介してなされる。ソフトウェアＡに対して、作成されたＡ／Ｖデータファイル１２の保存が指示される。この指示は，所定の形式で以てソフトウェアＡからＯＳ１１に対して伝達される。そして、ソフトウェアＡが有する鍵ｋｃがＯＳ１１に対して渡される。すると、ＯＳ１１によって、先ず、メモリ上に存在するＡ／Ｖデータファイル１２の著作権情報が読み出される。後述するが、この著作権情報は暗号化されているため，所定の方法で以て復号化される。

【００３２】解読された著作権情報からＣＧＭＳ情報が抽出され、上述の図４に示したフローチャートに従って、このＡ／Ｖデータファイル１２が保存可能であるかどうかが判断される。この判断の結果、保存可能であると判断されたら、このＡ／Ｖデータファイル１２がハードディスクの所定の領域に書き込まれ保存される。そして、ＯＳ１１によってこのファイル１２の書き込み確認がなされ、確認情報がソフトウェアＡに対して伝達され、この情報を受け取ったソフトウェアＡにおいて、ファイル１２の保存が正しく完了したとされる。

【００３３】ヘッダ部に含まれる著作権情報は、ユーザによって、例えばバイナリデータの編集が可能なエディタなどを用いて容易に書き換えられてしまうおそれがある。そこで、この発明においては、上述したように、この著作権情報を所定の方法で暗号化する。図６は、この著作権情報の暗号化の方法の一例を概略的に示す。例えば上述のソフトウェアＡでのＡ／Ｖデータの作成に伴い、著作権情報が作成される。この著作権情報には，例えば著作者名，データ作成日といった、このファイルに格納されるＡ／Ｖデータの著作権を主張するために必要な情報と、上述のＣＧＭＳ情報とが含まれる。

【００３４】この著作権情報が例えば所定の文字列からなる暗号化鍵ｋｃに基づき暗号化される。暗号化鍵ｋｃは、特定のソフトウェアに依存するもので、例えば，上

述のA／Vデータファイルを作成するソフトウェアAや、作成されたファイルを読み込み再生あるいは実行するソフトウェアBに対して入力されたユーザのパスワードPwに基づいて生成される。また、これらのソフトウェアが予めこの鍵kcを有しているとしてもよい。

【００３５】この鍵kcによる暗号化の例として、例えば鍵kcに基づく所定の方法で以て、著作権情報を構成する記号あるいは文字列に対して転字や換字を繰り返し行なう方法が挙げられる。暗号化された著作権情報がヘッダ部にプロパティ情報として格納されると共に、作成されたA／Vデータがデータ部に格納され、A／Vデータファイルが作成される。

【００３６】このA／Vデータファイルに含まれる、暗号化された著作権情報は、図７に概略的に示されるように、鍵kcで以て暗号化のときとは逆の手順で復号化される。すなわち、例えばソフトウェアBにおいて、A／Vデータファイルのヘッダ部に格納されたプロパティ情報が読み出され、このプロパティ情報に含まれる暗号化された著作権情報が抽出される。そして、ソフトウェアBが予め有している鍵kcが用いられ、鍵kcに基づき所定の方法で以て暗号化された著作権情報が復号化される。上述の、CGMSによるコピー世代制限は、この復号化された著作権情報に対してなされる。

【００３７】なお、これら図６および図７に示した著作権情報の暗号化／復号化の手順は、原理的なものであり、この実施の一形態に適用されるに止まらず、後述する変形例にも適用されるものである。

【００３８】図８は、上述の図６および図７に示した著作権情報の暗号化および復号化の手順を、この実施の一形態に適合させより具体的に示す。この例では、著作権情報を暗号化する際の暗号化鍵kcは、OS１１において、ユーザパスワードPwおよびマスタ鍵kmとに基づき生成される。

【００３９】ユーザパスワードPwは、例えば、ユーザによって指定される所定の文字列からなり、OS１１において、ログインするユーザに対して個別に設定される。また、このパスワードPwは、ソフトウェアAにおいて設定されるようにしてもよい。パスワードPwは、OS１１において設定された場合には、OS１１の起動毎、ソフトウェアAにおいて設定された場合には、ソフトウェアAの起動毎に、ユーザに対して入力が求められる。マスタ鍵kmは、所定の文字列からなり、例えばOS１１のコンピュータ１に対するインストールの際になされるユーザ登録によって設定される。

【００４０】OS１１によって、A／Vデータファイル１２のヘッダ部のプロパティ情報から暗号化された著作権情報が読み出される。この著作権情報は、OS１１において、上述の鍵kcに基づき復号化される。そして、復号化された著作権情報からCGMS情報が抽出され、このCGMS情報に基づきこのファイル１２の保存の禁止／許可が判断される。

【００４１】この場合、復号化された著作権情報に基づきこのファイル１２に対するアクセスそのものの禁止／許可を判断するようにもできる。これは、例えば、パスワードPwがソフトウェアAに対して設定された場合に、この著作権情報がソフトウェアAに渡され、ソフトウェアAにおいてパスワードPwとこの著作権情報とが照合され、その結果がOS１１に渡されることによってなされる。

【００４２】一方、ソフトウェアAにおいて作成されたA／Vデータに対してCGMS情報が設定され、A／Vデータファイルとして保存される際に、OS１１において、鍵kcに基づいて著作権情報の暗号化がなされる。

【００４３】この実施の一形態では、A／Vデータファイルの著作権保護のためのCGMS情報の、例えば照合や書き換えといった処理は、OS１１においてなされる。このOS１１上では、作成される全てのファイルに対して著作権情報が設定され、全てのファイル操作の際に、この設定された著作権情報の照合などの処理がなされる。そこで、この著作権保護システムに対応していない、他のOS上で作成されたファイル操作に対して互換性を持たせる必要がある。

【００４４】図９は、このファイルの互換性を考慮した、OS１１におけるファイルに対するアクセスのフローチャートを示す。ファイルに対するアクセスがなされると、先ず、ステップS１０において、このファイルがOS１１による著作権保護システムに対応しているかどうかが判断される。この判断は、例えば、OS１１において著作権保護システムに対応しているファイルにはヘッダ部にその旨を示すフラグなどを記し、このフラグの有無を調べることによって行なうことができる。また、ヘッダ部の著作権情報そのものの有無を調べるようにしてもよい。

【００４５】若し、著作権保護システムに対応していないと判断されたら、このファイルに対する著作権保護の手段はとられず、ステップS１７においてファイルの保存がなされる。

【００４６】一方、ステップS１０でファイルが著作権保護システムに対応していると判断されたら、処理はステップS１１に移行する。そして、ステップS１１において、このファイルの著作権情報が読み出され、復号化される。この復号化は、例えばOS１１から所定のソフトウェア（例えば上述のソフトウェアAあるいはB）に対して暗号化鍵kcを要求し、この要求に対してそのソフトウェアから渡された鍵kcに基づいてなされる。著作権情報の復号化がなされると、処理はステップS１２に移行する。

【００４７】ステップS１２では、復号化された著作権情報からCGMS情報が抽出される。そして、次のステップS１３で、CGMS情報の状態が判断される。若

し、CGMS＝'11'であれば、処理はステップS14に移行し、上述のCGMSの定義に従いファイル保存は不可であるとされる。また若し、CGMS＝'00'であれば、定義に従いファイル保存が可能とされるため、処理はステップS16に移行する。さらに若し、CGMS＝'10'であれば、処理はステップS15に移行し、CGMS情報が'11'に書き換えられる。そして、処理は次のステップS16に移行する。

【0048】ステップS16において、著作権情報が暗号化される。この暗号化は、例えばOS11から所定のソフトウェアに対して暗号化鍵kcを要求し、この要求に対してそのソフトウェアから渡された鍵kcに基づいてなされる。暗号化がなされると、ファイルのヘッダ部に含まれる著作権情報がこのステップS16で暗号化された著作権情報とされる。そして、次のステップS17で、このファイルが保存される。

【0049】なお、上述の説明では、ネットワーク2に接続されたコンピュータ1および3a，3b，・・・のそれぞれには、全て同一のOS11が搭載されているとしたが、これはこの例に限定されない。コンピュータ1および3a，3b，・・・に対してそれぞれ異なるOSが搭載されている場合でも、互いに共通のプロトコルで以てデータ通信を行なうことができれば、この発明による著作権保護システムを適用することができる。

【0050】また、上述のフローチャートは、著作権保護システムに対応していないファイルの互換性が考慮されたものだが、この処理を応用することによって、著作権保護を必要とされないファイルを選択的に設定することができる。

【0051】A／Vデータファイルは、データファイルとしてのコピーが行なわれるだけでなく、例えばコンピュータによってこのファイルが再生あるいは実行され、アナログ方式やディジタル方式のビデオ信号とされ外部に出力されることも考えられる。この出力されたビデオ信号は、例えばアナログビデオテープレコーダによって記録され、それによりA／Vデータに対する著作権の侵害が生じる可能性がある。したがって、このような場合における著作権保護についても考慮する必要がある。

【0052】図10は、A／Vデータファイルから再生されたA／Vデータがコンピュータ外部に対して出力される場合の、データ変換の方法を概念的に示す。ここでは、A／VデータがアナログRGB信号に変換され出力される例を示す。図示せずとも、ソフトウェアAによってA／Vデータファイル12が再生され、A／Vデータが出力される。このA／Vデータは、エンコーダ20に供給され、D／A変換されると共に、例えばRGBの各色の信号からなるコンポーネントビデオ信号とされる。このコンポーネントビデオ信号のうち、例えばR信号が加算器22の一方の入力端に対して供給される。

【0053】この加算器22は、他方の入力端に供給された信号の、一方の入力端に供給されたビデオ信号に対する加算を、ビデオ信号に同期して所定のタイミングで以て制御することができる。これは、例えばエンコーダ20において、A／Vデータをビデオ信号に変換する際に用いられたタイミング信号に基づき生成された制御信号が、この加算器22に供給されることによってなされる。

【0054】一方、ソフトウェアAあるいはOS11によって、A／Vデータファイルから著作権情報が読み出される。この著作権情報が鍵kcによって復号化され、APS情報が抽出される。そして、このAPS情報に基づきアナログコピー制限用信号が生成され、生成されたこの信号は、加算器22の他方の入力端に供給される。加算器22では、この信号を、一方の入力端に供給されているR信号の、例えば水平あるいは垂直ブランキング期間に加算する。

【0055】図示しないが、このアナログビデオ信号は、モニタに対して供給され映出されると共に、例えばAPSに対応したRGB信号／コンポジットビデオ信号変換器に供給される。コピー制限用信号は、ブランキング期間に重畳されているため、モニタへの映出には直接的な影響はない。しかしながら、APSに対応したRGB信号／コンポジットビデオ信号変換器を介して外部にコンポジットビデオ信号として出力された場合、上述の図3Bに一例が示される、APS情報の定義に基づいたコピー防止用信号がこのビデオ信号に対して重畳または付加される。そのため、このビデオ信号をビデオテープなどに記録しても、正常な画像として再生することができず、結果的にA／Vデータに対する著作権を保護することができる。

【0056】なお、A／Vデータファイルが再生されディジタル画像データとして外部に出力される場合には、著作権情報から抽出されたCGMS情報およびAPS情報とがそのまま伝送され、例えばディジタルビデオカセットレコーダによって、テープの所定の領域に記録される。したがって、この場合でも容易にコピー防止の効果を得ることができる。

【0057】次に、この発明の実施の一形態の変形例について説明する。図11は、この変形例におけるA／Vデータファイル構造の一例を概略的に示す。この変形例においては、データ部に格納されたA／Vデータが所定の暗号化鍵kdに基づき暗号化され、この鍵kdがA／Vデータファイルのヘッダ部の著作権情報と共に、所定の暗号化鍵に基づき暗号化される。この変形例では、このようにA／Vデータそのものを暗号化することにより、より強固にA／Vデータの著作権保護を行なうものである。

【0058】図12は、この変形例によるA／Vデータファイルの暗号化の方法の一例を概略的に示す。この例においては、A／Vデータファイル供給側からユーザに

対して配布される顧客管理鍵ｋｕを用いて、著作権情報およびデータ暗号化鍵ｋｄの暗号化を行なう。

【００５９】Ａ／Ｖデータは、このデータの供給側で管理しているデータ暗号化鍵ｋｄに基づいて暗号化される。この暗号化には、例えば、鍵ｋｄに基づいた所定の規則に従って転字や換字を繰り返すことによってなされる。この暗号化されたＡ／Ｖデータは、Ａ／Ｖデータファイルのデータ部に格納される。また、このＡ／Ｖデータの暗号化に用いられた鍵ｋｄは、著作権情報と共に、Ａ／Ｖデータの供給側において管理される顧客管理鍵ｋｕに基づき暗号化される。この顧客管理鍵ｋｕは、例えばこのＡ／Ｖデータの供給を受けた顧客のそれぞれに対して設定され、Ａ／Ｖデータ供給側から渡される。こうして暗号化された著作権情報および鍵ｋｄとは、プロパティ情報としてＡ／Ｖデータファイルのヘッダ部に格納される。

【００６０】図１３は、この変形例によるＡ／Ｖデータファイルの復号化の方法の一例を概略的に示す。Ａ／Ｖデータの供給側からユーザに対して渡されたＡ／Ｖデータファイルにおいて、ヘッダ部が読み込まれ、暗号化された著作権情報およびデータ暗号化鍵ｋｄが抽出される。また、Ａ／Ｖデータ供給側からユーザに対して、予め顧客管理鍵ｋｕが渡される。ヘッダ部から抽出された暗号化された著作権情報および鍵ｋｄがこの顧客管理鍵ｋｕによって復号化される。そして、この復号化された顧客管理鍵ｋｕによって、データ部に格納された、暗号化されたＡ／Ｖデータが復号化される。

【００６１】この例のように、顧客管理鍵ｋｕを用いることによって、Ａ／Ｖデータ供給側は、ユーザに対してＡ／Ｖデータファイルの使用を限定することができ、Ａ／Ｖデータ供給側における顧客管理を行なうことができる。そのため、この顧客管理鍵ｋｕを用いた方法は、例えば大量生産されるＡ／Ｖデータファイルに対して用いて好適なものである。

【００６２】一方、上述の実施の一形態における著作権保護の方法は、例えば個人の創作に関する著作権の保護に対して用いて好適である。

【００６３】なお、この変形例は、この例に限らず、例えば顧客管理鍵ｋｕの代わりに、上述の実施の一形態において用いられた暗号化鍵ｋｃを用いることも可能である。勿論この場合には、Ａ／Ｖデータ供給側による顧客管理は、厳密には行なわれない。

【００６４】上述の実施の一形態およびその変形例とにおいては、著作権情報処理に対応したＯＳに対してこの発明が適用されるように説明したが、これは、この例に限定されるものではない。図１４は、この発明の別の変形例として、著作権情報処理に対応していないＯＳに対してこの発明が適用された際の、ソフトウェアＡ’，ＯＳ１１’，Ａ／Ｖデータファイル１２間における処理の推移を概略的に示す。なお、この別の変形例は、上述の実施の一形態およびその変形例とによる何方のファイル構造に対しても適用可能なものである。

【００６５】この別の変形例においては、上述の実施の一形態およびその変形例ではＯＳ１１においてなされていた、Ａ／Ｖデータファイルからの著作権情報の読み出しおよび読み出された著作権情報の解読を、ソフトウェアＡ’上で行なう。Ａ／Ｖデータファイル１２は、当初図示されないメモリ上に存在し、ソフトウェアＡ’に対してこのファイル１２の保存を指示することによって、このメモリから例えば図示されないハードディスクに対して保存される。なお、これはこの例に限られず、例えばハードディスクの第１の領域から第２の領域へのＡ／Ｖデータファイルのコピー、あるいはネットワークを介して伝送されたＡ／Ｖデータの保存などにも適用できる。

【００６６】ソフトウェアＡ’に対して、作成されたＡ／Ｖデータファイル１２の保存が指示される。この指示に基づき、Ａ／Ｖデータファイル１２のヘッダ部からプロパティ情報が読み出され、読み出されたこのプロパティ情報から著作権情報が抽出される。この著作権情報は、例えばソフトウェアＡ’が固有に有している暗号化鍵ｋｃによって暗号化されている。この鍵ｋｃに基づき著作権情報が復号化され、解読される。

【００６７】なお、著作権情報の暗号化に用いられた暗号化鍵は、この例のような暗号化鍵ｋｃに限られない。例えば、上述の、Ａ／Ｖデータファイル供給側からユーザに対して渡された顧客管理鍵ｋｕをこの暗号化鍵として用いるようにもできる。

【００６８】解読された著作権情報からＣＧＭＳ情報が抽出され、上述の図４に示したフローチャートに従って、このＡ／Ｖデータファイル１２が保存可能であるかどうかが判断される。この判断の結果、保存可能であると判断されたら、ＯＳ１１’によって、このＡ／Ｖデータファイル１２が例えばハードディスクの所定の領域に書き込まれ保存される。そして、ＯＳ１１’によってこのファイル１２の書き込み確認がなされ、確認情報がソフトウェアＡ’に対して伝達され、この情報を受け取ったソフトウェアＡ’において、ファイル１２の保存が正しく完了したとされる。

【００６９】

【発明の効果】以上説明したように、この発明によれば、Ａ／Ｖデータファイルのプロパティ情報に、著作権保護を行なうための著作権情報が含まれる。そのため、コンピュータ上で扱われるＡ／Ｖデータに対しても、著作権保護の機構を導入することができ、著作権の侵害が防止される効果がある。

【００７０】また、この発明によれば、著作権情報に対してコピーの世代制限を制御するＣＧＭＳ情報が含まれ、ディジタルＡ／Ｖ機器などで既に導入されているものと同一の概念でＡ／Ｖデータの著作権保護が行なわれ

る。そのため、コンピュータ上のA／Vデータとディジタル A／V機器との間で、著作権保護の考え方に整合性がとれる効果がある。

【0071】さらに、この発明によれば、著作権情報は、暗号化されているため、ユーザによる不正な書き換えなどから保護され、安全性が高いという効果がある。

【0072】さらにまた、この発明によれば、OSにおいてファイルの更新や保存の際に著作権情報が含まれるプロパティ情報を参照するようにされているため、アプリケーションソフトウェアだけで同様の処理を行なう場合に比べ、著作権保護の確実性がより高まるという効果がある。

【0073】また、この発明による著作権保護のための処理は、高々数バイトのデータをソフトウェアあるいはOS上でハンドリングするだけで行なわれるので、著作権保護のために新たに発生するコストは無視できる程度のものであるという効果がある。

【0074】さらに、この発明による著作権情報は、A／Vデータファイルのプロパティ情報として扱われるため、ファイルから削除することができず、より確実に著作権保護を行なうことができるという効果がある。

【0075】また、この発明による著作権情報は、既に存在するディジタルA／V機器における著作権保護と共通の考えに基づいて設定されている。そのため、この発明によるA／Vデータは、ディジタルA／V機器とのインターフェイス上にそのまま伝送することができるという効果がある。

【図面の簡単な説明】

【図1】説明において想定されるシステム構成を概略的に示す図である。

【図2】実施の一形態におけるA／Vデータファイル構造の一例を概略的に示す図である。

【図3】CGMS情報およびAPS情報の一例を示す略＊線図である。

【図4】CGMSによるコピー世代制限のフローチャートである。

【図5】A／Vデータファイルを保存する際の、ソフトウェア，OS，およびA／Vデータファイル間における処理の推移を概略的に示す図である。

【図6】著作権情報の暗号化の方法の一例を概略的に示す図である。

【図7】著作権情報の復号化の一例を概略的に示す図である。

【図8】著作権情報の暗号化および復号化の手順をより具体的に示す図である。

【図9】ファイルの互換性を考慮した、OSにおけるファイルに対するアクセスのフローチャートである。

【図10】A／Vデータファイルを外部出力する場合のデータ変換の方法を概念的に示す図である。

【図11】変形例におけるA／Vデータファイル構造の一例を概略的に示す図である。

【図12】顧客管理鍵kuを用いた場合の、A／Vデータファイルの暗号化の方法の一例を概略的に示す図である。

【図13】顧客管理鍵kuを用いた場合の、A／Vデータファイルの復号化の方法の一例を概略的に示す図である。

【図14】OSが著作権情報処理に対応していない場合の、ソフトウェア，OS，A／Vデータファイル間における処理の推移を概略的に示す

【符号の説明】

1，3a，3b・・・コンピュータ、11・・・OS、12・・・A／Vデータファイル、A，B・・・アプリケーションソフトウェア、kc・・・暗号化鍵、kd・・・データ暗号化鍵、km・・・マスタ鍵、ku・・・顧客管理鍵、Pw・・・ユーザパスワード

【図3】

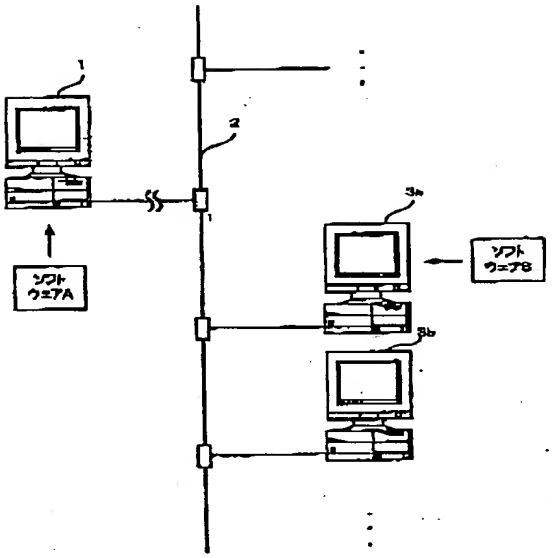
A

| CGMS | | 定義 |
|---|---|---|
| 1 | 1 | コピー不可 |
| 1 | 0 | コピー1世代可能 |
| 0 | 1 | 未使用 |
| 0 | 0 | コピー可能 |

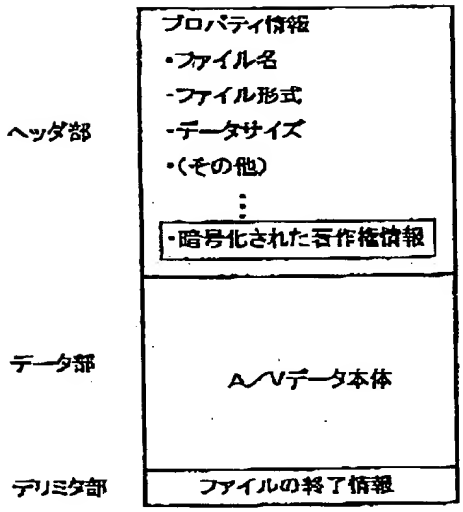
B

| フラグ | | 定義 |
|---|---|---|
| 0 | 0 | OFF |
| 0 | 1 | PSP ON |
| 1 | 0 | PSP ON, 2ラインスプリットバースト-ON |
| 1 | 1 | PSP ON, 4ラインスプリットバースト-ON |

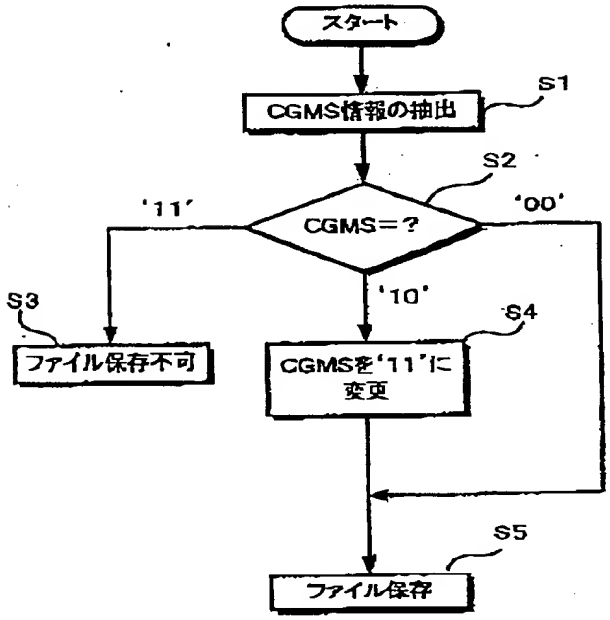
【図１】


1
2
3a
3b
ソフトウェアA
ソフトウェアB

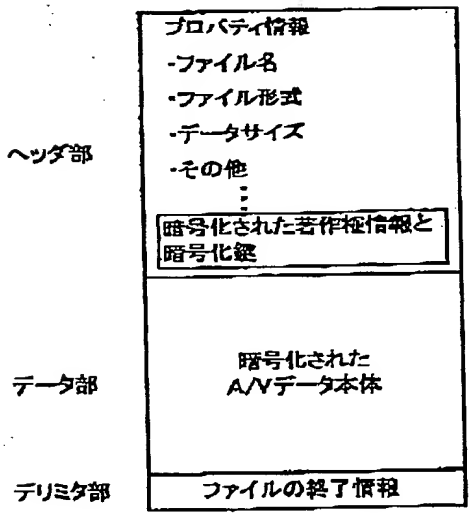
【図２】


ヘッダ部
データ部
デリミタ部
プロパティ情報
・ファイル名
・ファイル形式
・データサイズ
・(その他)
・暗号化された著作権情報
A/Vデータ本体
ファイルの終了情報

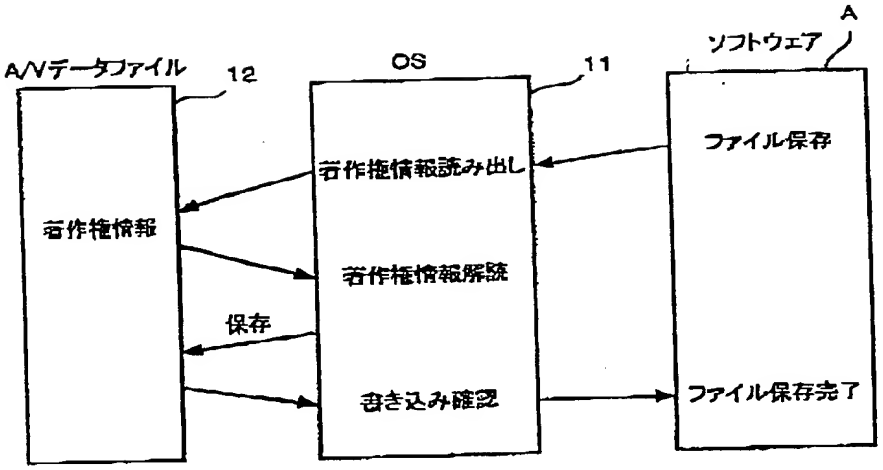
【図４】


スタート
CGMS情報の抽出
S1
CGMS＝？
S2
'11'
'00'
'10'
S3
ファイル保存不可
CGMSを'11'に変更
S4
S5
ファイル保存

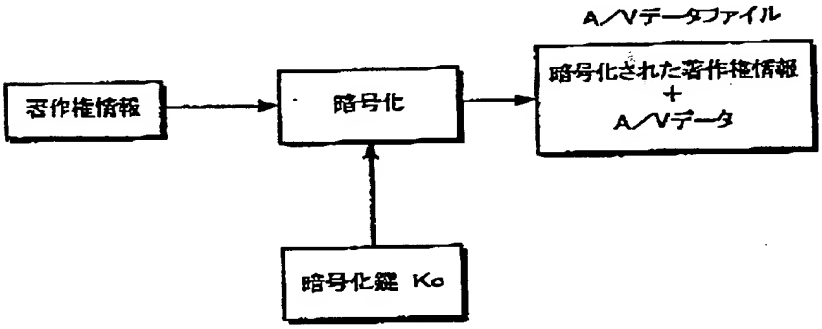
【図１１】


ヘッダ部
データ部
デリミタ部
プロパティ情報
・ファイル名
・ファイル形式
・データサイズ
・その他
暗号化された著作権情報と暗号化鍵
暗号化されたA/Vデータ本体
ファイルの終了情報

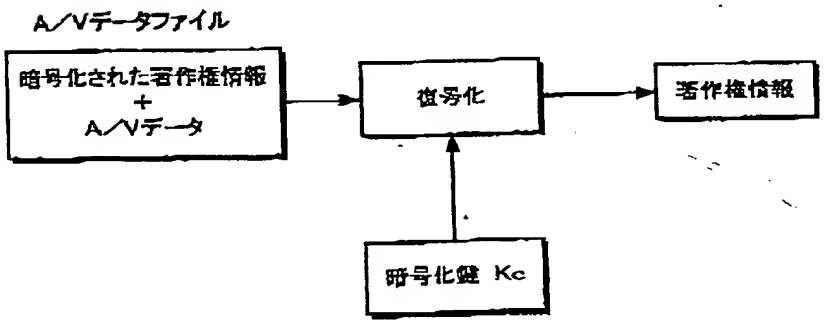
【図5】


A
ソフトウェア
A/Vデータファイル
12
OS
11
ファイル保存
著作権情報読み出し
著作権情報
著作権情報解読
保存
書き込み確認
ファイル保存完了

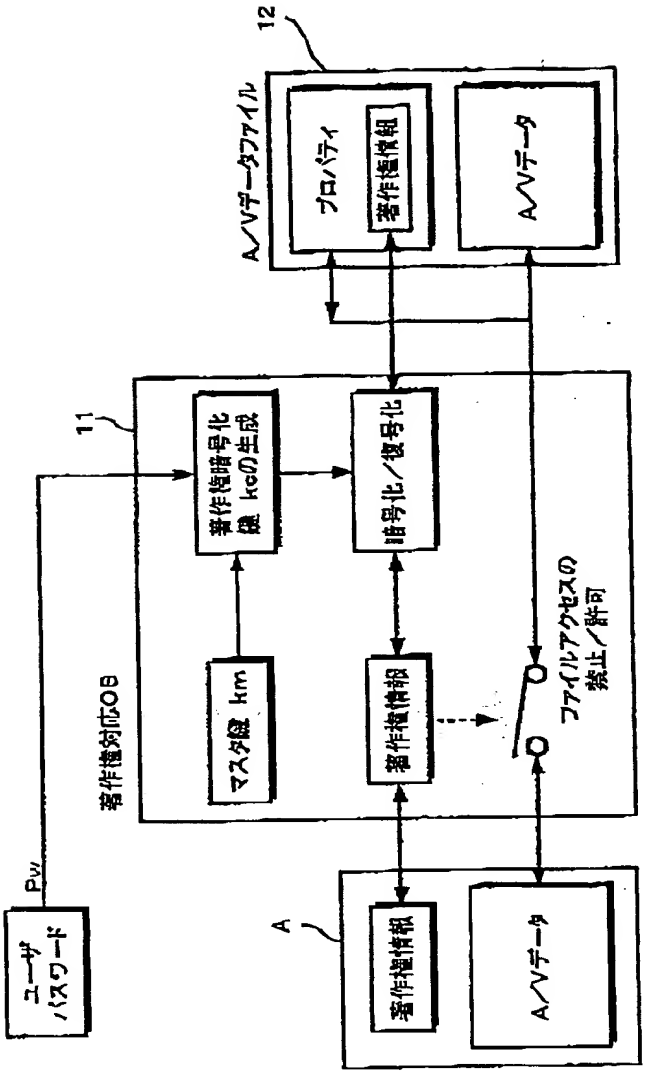
【図6】


A/Vデータファイル
著作権情報
暗号化
暗号化された著作権情報
+
A/Vデータ
暗号化鍵 Kc

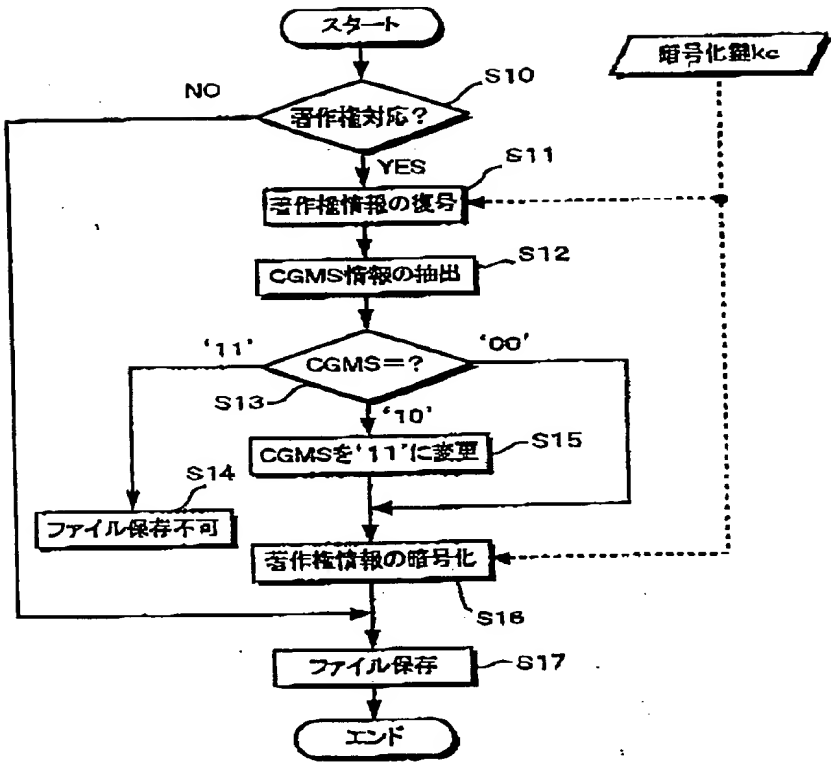
【図7】


A/Vデータファイル
暗号化された著作権情報
+
A/Vデータ
復号化
著作権情報
暗号化鍵 Kc

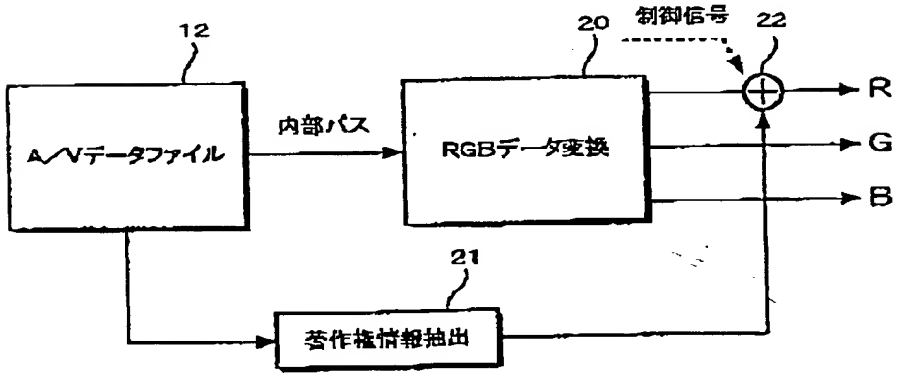
【図8】


12
A/Vデータファイル
プロパティ
著作権情報
A/Vデータ
11
著作権暗号化鍵 kcの生成
暗号化／復号化
マスター鍵 km
著作権情報
ファイルアクセスの禁止／許可
著作権対応OS
Pw
ユーザパスワード
A
著作権情報
A/Vデータ

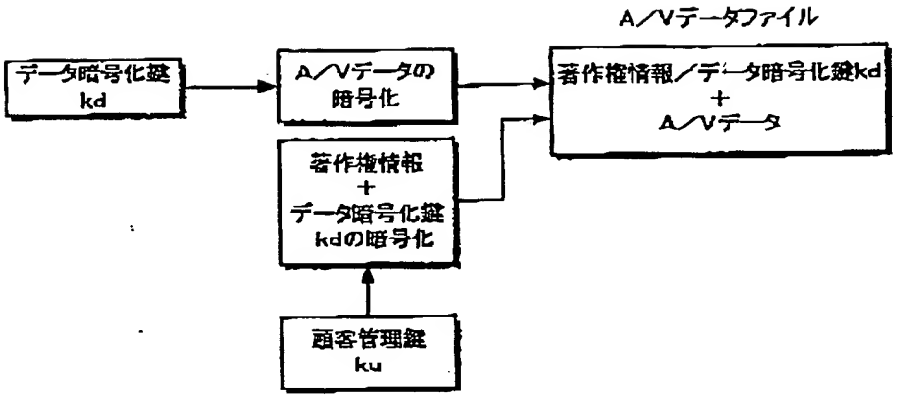
【図9】


スタート
暗号化鍵kc
NO
S10
著作権対応？
YES
S11
著作権情報の復号
S12
CGMS情報の抽出
'11'
CGMS＝？
'00'
S13
'10'
CGMSを'11'に変更
S15
S14
ファイル保存不可
著作権情報の暗号化
S16
ファイル保存
S17
エンド

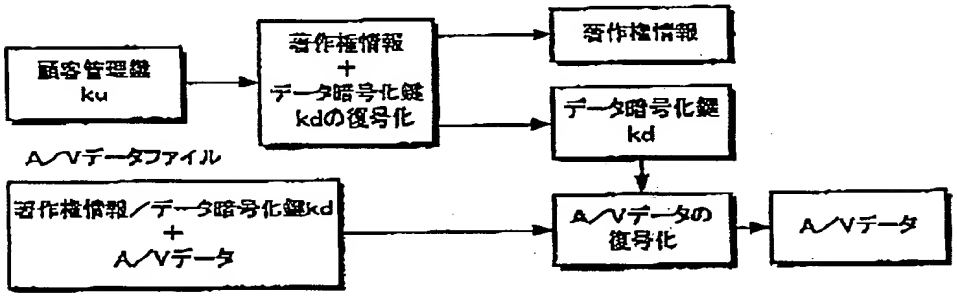
【図10】


12
20
制御信号
22
A／Vデータファイル
内部バス
RGBデータ変換
R
G
B
21
著作権情報抽出

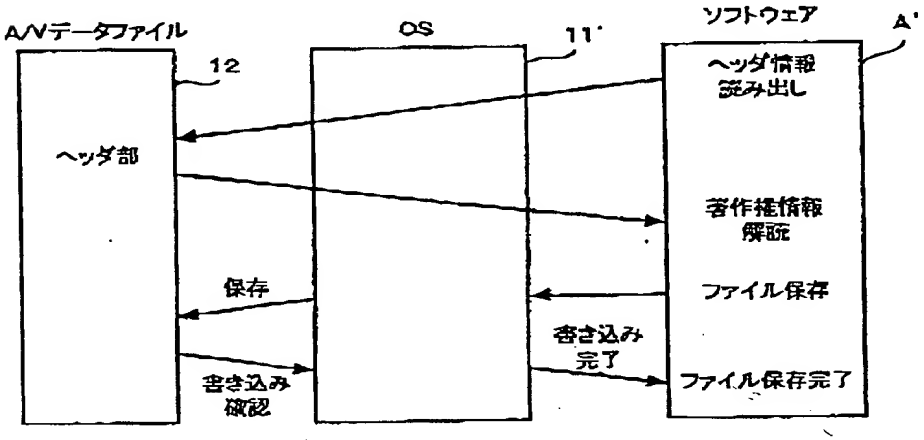
【図12】


A／Vデータファイル
データ暗号化鍵
kd
A／Vデータの
暗号化
著作権情報／データ暗号化鍵kd
＋
A／Vデータ
著作権情報
＋
データ暗号化鍵
kdの暗号化
顧客管理鍵
ku

【図13】


顧客管理鍵
ku
著作権情報
＋
データ暗号化鍵
kdの復号化
著作権情報
データ暗号化鍵
kd
A／Vデータファイル
著作権情報／データ暗号化鍵kd
＋
A／Vデータ
A／Vデータの
復号化
A／Vデータ

【図14】


A／Vデータファイル
OS
11'
ソフトウェア
A'
12
ヘッダ部
ヘッダ情報
読み出し
著作権情報
解読
保存
ファイル保存
書き込み
完了
書き込み
確認
ファイル保存完了

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１４年６月７日（２００２．６．７）

【公開番号】特開平１０－１０８１４８
【公開日】平成１０年４月２４日（１９９８．４．２４）
【年通号数】公開特許公報１０－１０８２
【出願番号】特願平８－２７７１３０
【国際特許分類第７版】
H04N 7/08
7/081
G06F 15/00 330
G09C 1/00 660
H04N 7/167
【ＦＩ】
H04N 7/08 Z
G06F 15/00 330 Z
G09C 1/00 660 D
H04N 7/167 Z

【手続補正書】
【提出日】平成１４年３月１４日（２００２．３．１４）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　作成されたディジタルデータの著作権保護方法において、
著作権情報を暗号化鍵に基づき暗号化する暗号化のステップと、
上記暗号化された著作権情報をファイルの所定の領域に格納する著作権情報格納のステップと、
上記ファイルに対してアクセスし、上記暗号化された著作権情報を復号化する復号化のステップと、
上記復号化された著作権情報に基づき著作権保護を行なう著作権保護のステップと
を有することを特徴とするディジタルデータの著作権保護方法。
【請求項２】　請求項１に記載のディジタルデータの著作権保護方法において、
上記所定の領域は、上記ファイルの属性情報を格納する領域であることを特徴とするディジタルデータの著作権保護方法。
【請求項３】　請求項１に記載のディジタルデータの著作権保護方法において、
上記ファイルに格納される上記ファイルのデータ本体を他の暗号化鍵に基づき暗号化する他の暗号化のステップと、
上記データ本体を上記他の暗号化鍵に基づき復号化する他の復号化のステップと
をさらに有し、
上記暗号化のステップは、上記著作権情報と上記他の暗号化鍵とを上記暗号化鍵で暗号化することを特徴とするディジタルデータの著作権保護方法。
【請求項４】　作成されたディジタルデータの著作権保護システムにおいて、
著作権情報を暗号化鍵に基づき暗号化する暗号化手段と、
上記暗号化された著作権情報をファイルの所定の領域に格納する著作権情報格納手段と、
上記ファイルに対してアクセスし、上記暗号化された著作権情報を復号化する復号化手段と、
上記復号化された著作権情報に基づき著作権保護を行なう著作権保護手段とを有することを特徴とするディジタルデータの著作権保護システム。